OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

Follow-up report

Left untreated: Security gaps in BC's public health database

BACKGROUND

Six months after the release of Investigation Report 22-02, the OIPC began reviewing the Provincial Health Services Authority's (PHSA) implementation of the seven recommendations made in that report. This follow-up report details how the PHSA has taken positive steps to address those recommendations.

THE OIPC

Established in 1993, the Office of the Information and Privacy Commissioner provides independent oversight of BC's access and privacy laws.

IR 22-02

The initial investigation found major gaps in the technological controls the PHSA had in place to protect personal information stored in the Provincial Public Health Information System.

STATUS

Two recommendations have been fully implemented, three have been subtantially implemented, and the remaining two have been partially implemented, with progress continuing .

THE SYSTEM

The System collects significant volumes of sensitive personal information about all British Columbians, to facilitate the delivery of healthcare and to manage outbreaks of communicable diseases.

READ MORE

Check out *Investigation Report 22-02 Left untreated: Security gaps in BC's public health database* to learn more about the seven recommendations made to address the System's identified privacy and security risks.

https://www.oipc.bc.ca/investigation-reports/3736

> I am pleased to report that the Provincial Health Services Authority (PHSA), the body tasked with operating the Provincial Public Health Information System, has taken meaningful steps to strengthen the privacy and security of the System.

FROM THE COMMISSIONER

As digital innovation continues to transform health care provided in Canada and abroad, British Columbians find increasing amounts of their sensitive personal information being collected and stored within digital systems. From personal health numbers to records relating to individuals' mental health status, British Columbia's Provincial Public Health Information System stores large amounts of sensitive information about those of us accessing health care and communicable disease services.

Not only is the information stored within the Provincial Public Health Information System highly personal and sensitive, but the security of the System itself is also critical to British Columbians ability to access quality care. It was for this reason that in 2022 my office initiated an investigation into the System's privacy and security protections.

In December 2022, my office published the initial investigation report which included seven recommendations to ensure the continued availability of the province's health care system to enhance the protection of individuals' information and privacy rights.

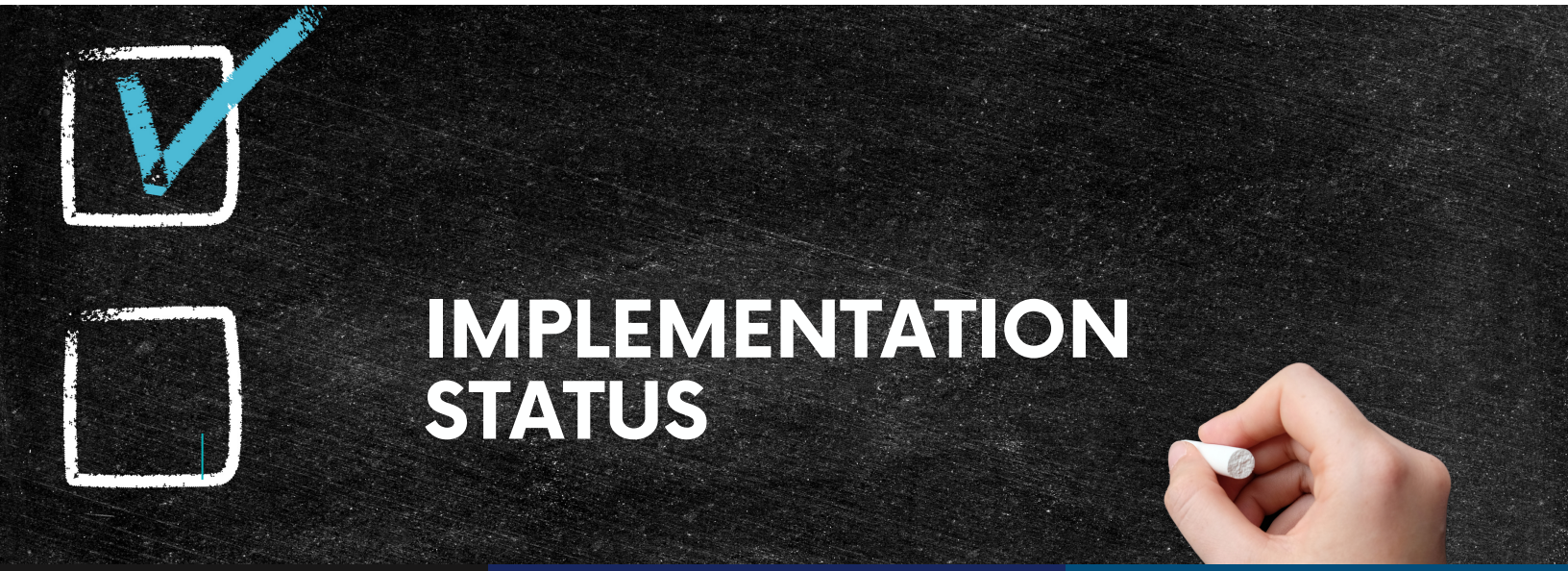
I am pleased to report that the Provincial Health Services Authority (PHSA), the body tasked with operating the Provincial Public Health Information System, has taken meaningful steps to strengthen the privacy and security of the System...

(See page 2 of the report for the full Commissioner's Message)

Follow-up report

Left untreated: Security gaps in BC's public health database

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA



FULLY

Recommendations 3, 4

Recommendation 3:
Implement an ongoing application vulnerability management program to monitor for risk exposures related to unpatched software, and regularly report those to senior management.

Recommendation 4:
Evaluate implementing the encryption of personal information within the Database.

SUBSTANTIALLY

Recommendations 1, 2, 5

Recommendation 1:
Acquire, configure, and deploy privacy-tailored security information and event management technology that is supported by appropriate staffing to maintain the technology and to conduct privacy investigations.

Recommendation 2:
Produce and maintain a comprehensive written security architecture document that includes system security requirements, controls design documentation and operations manuals for each component of the System. Ensure the document is signed and approved by senior officials at the PHSA and use it to form the basis for an annual security audit.

Recommendation 5:
Conduct penetration testing at least one per year, then report the results and mitigation plans to the Ministry within three months of the completion of the penetration test.

PARTIALLY

Recommendations 6, 7

Recommendation 6:
Ensure that only secure desktops can access the System, or ensure the security of the System cannot be compromised by unsecure desktop environments with access to the System.

Recommendation 7:
Conduct an Identity Risk Assessment to determine the appropriate level of Identity Assurance required of the System. The PHSA should ensure that all organizations accessing the System use an authentication solution that meets the assurance level required.

A MESSAGE FROM THE COMMISSIONER

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

https://youtu.be/AmJUdqCDI-E

READ MORE

Check out the full follow-up report at:
https://www.oipc.bc.ca/investigation-reports/